AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

1 Dell Precision M 4800 Laptops
Service Tag 427TF12, located at 13 Bataan Blvd, Santa Fe, New Mexico

Case No. 17-mR-538

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A, incorporated by reference

located in the ________ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B, incorporated by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☑ evidence of a crime;
☑ contraband, fruits of crime, or other items illegally possessed;
☑ property designed for use, intended for use, or used in committing a crime;
□ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1343	Wire Fraud
18 U.S.C. 1001	False Statements

The application is based on these facts:
See affidavit attached

☑ Continued on the attached sheet.
□ Delayed notice of ____ days (give exact ending date if more than 30 days: ________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

R Vargas
Applicant's signature

Robert Vargas, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 06/22/2017

Karen B Molzen
Judge's signature

City and state: Albuquerque, New Mexico

Karen B. Molzen
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Robert Vargas, being first duly sworn, hereby depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – electronic devices – which are currently in the possession of the Department of Homeland Security, Emergency Management Information Technology Office, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent (SA) with the United States Department of Homeland Security (DHS) Office of Inspector General (OIG), Alpine, TX, and have been since January 2011. Prior to the DHS OIG your affiant was employed with the Harlingen Police Department, where he was assigned to the Brownsville, TX., Drug Enforcement Administration (DEA) as a Task Force Officer. Prior to this, your affiant honorably served in the United States Air Force for 9 years as a Criminal Investigator with Security Forces and the Air Force Office of Special Investigations. Affiant is currently assigned to investigate violations of federal law as it pertains to employees and/or contractors of the DHS. As a Special Agent with the DHS OIG, I attended 16 weeks of training at the Federal Law Enforcement Training Center in Glynco, Georgia, where I received instruction in the investigation of federal crimes. Affiant has training and experience in the area of financial crimes and the investigation of contract fraud. As a Special Agent with DHS OIG, and in prior law enforcement capacities, Affiant participated in numerous criminal investigations of alleged violations of both state and federal laws.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a Dell Precision M4800 laptop computer bearing service tag 427TF12, herein after the "Device." The Device is currently located at the Department of Homeland Security, Emergency Management Information Technology Office, 13 Bataan Blvd, Santa Fe, NM, 87508.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. In September 2015, the Department of Homeland Security Office of Inspector General received an allegation that the New Mexico Task Force I (NM-TF 1), which is part of the Federal Emergency Management Agency (FEMA) Urban Search and Rescue team, located in Albuquerque, NM, produced and provided fraudulent training certificates showing that its task force members had completed FEMA's on-line introductory ethics training course. When the provided certificates were checked against the FEMA's Emergency Management Institute database, the information revealed that the courses had not been completed and/or the dates differed from the information on the database. The fraudulent certificates were provided to FEMA by NM-TF 1 in order to receive federal program funds and to certify NM-TF 1 in order for them (NM-TF 1) to respond to disaster areas. As the investigation proceeded, a source of information (SOI) came forward and provided information. The SOI said that he/she was tasked with assisting Dante Halleck, the former training manager for NM-TF 1, with getting the task force in compliance with training requirements in order for NM-TF 1 to be able to deploy to disaster areas and receive its yearly funding from FEMA. The SOI stated that as he/she started going through the training folders of the task force members he/she observed that many members lacked the FEMA ethics training. The SOI then approached Halleck and made him aware of the lack of training certificates. Halleck responded that he was in possession of a FEMA certificate template that

Halleck obtained from a person in Santa. Fe, NM, and that he would manufacture the training certificates. Halleck then asked the SOI for names of persons who were lacking the ethics training and proceeded to input the names into his laptop and print out a fraudulent certificate to be placed in the training file.

7. Based on the aforementioned information, Halleck's laptop was confiscated pursuant to a federal search warrant. The laptop was analyzed by the DHS OIG Digital Forensic and Analysis Unit. Moreover, on February 10, 2017, the DHS OIG obtained a voluntary statement from Halleck in which he stated that the FEMA training web site which administered the on-line training for several of the training certifications lacked positive control on both ends. He stated that this was common knowledge amongst the NM-TF 1 staff and through-out the USAR national team. Halleck stated that because of this lack of positive control, anyone could enter the web-site with a member's student identification number and take the on-line training with no way of verifying that the actual member took it. Halleck stated that under NM-TF 1 Bureau Chief Gregory Lee's direction, he and NM-TF 1 Clerical Specialist Darlene Torres would access the FEMA website with their Devices and take the FEMA training courses for various members to generate the certificates. Halleck stated that Lee would often do the same with his Device. Halleck stated that Lee utilized his Device to forward the FEMA link which contained the completion of on-line training and certificates for NM-TF 1 members.

8. Based on the facts stated above, there is probable cause to believe that evidence, fruits or instrumentalities of the offense of 18 U.S.C. §§ 1343, Wire Fraud and/or U.S.C 1001, False Statement will be found within the Device which was utilized by Gregory Lee.

9. NM-TF 1 is a team of state sponsored employees who receive funding and technical direction on standard operating procedures, equipment, training, and exercise requirements from the Federal Emergency Management Agency Search and Rescue Program, to assist in disaster related

operations. The task force had been out of compliance for several years due to a majority of its task force members not meeting FEMA's training standards and/or certification requirements. However, FEMA continued to fund NM-TF 1 in order for NM-TF 1 to attain compliance and certify its task force members to deploy to disaster areas. In September 2015, based on significant non-compliance issues with the Code of Federal Regulations requirements, cooperative agreements and subordinate polices over many years, FEMA terminated the Memorandum of Agreement with the State of New Mexico resulting in the disbandment of the NM-TF 1.

10. On March 30, 2017, Gregory Lee's and Darlene Torres' USAR laptops were confiscated pursuant to a federal search warrant. The laptops are currently being analyzed by the DHS OIG Digital Forensic and Analysis Unit.

11. On May 31, 2017, Mark Rivera, IT Systems Manager with DHS Emergency Management, New Mexico, contacted your affiant and advised that on May 25, 2017, he discovered an additional laptop that was assigned to Gregory Lee while conducting an on-site IT inventory at the USAR facility in Albuquerque, NM. Rivera stated that he recognized the Dell Precision M4800 which contained a service Tag 427TF12 as the newest laptop that he assigned to Lee after he was experiencing issues with his original laptop. Rivera described the laptop with service tag 427TF12 as a replacement and the last laptop that was used by Lee before resigning. Rivera took custody of the laptop and transported it to the Department of Homeland Security, Emergency Management Information Technology Office, located at 13 Bataan Blvd, Santa Fe, NM.

TECHNICAL TERMS

12. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Laptop Computer: A laptop computer is a portable computer light and small enough to sit on a person's lap. A laptop computer can be powered by battery or plugged into the wall. The main utility of a laptop computer is that it allows a person to travel with their computing resource.

13. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a mobile workstation which contains an i5-4210 Processor, 8 gigabytes of memory, 500 gigabyte hard drive and an Intel dual band wireless Bluetooth and mini card. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

14. Based on my knowledge, training, and experience, I know that electronic device can store information for long periods of time. Similarly, things that have been viewed via electronic mail or the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

a. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

15. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

16. Manner of execution. Because this warrant seeks only permission to examine devices already in official possession, the execution of this warrant does not involve the physical intrusion onto premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

17. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Robert Vargas, Special Agent
Department of Homeland Security
Office of Inspector General

Sworn to and subscribed before me on this ~~XX~~ 22 day of ~~XX~~ June, 2017

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched consists of a Dell Precision M4800 Laptops, bearing service tag 427TF12, hereinafter the "Device." The Device is currently located at 13 Bataan Blvd, Santa Fe, New Mexico.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

KBM

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §§ 1001 and/or 1343 and involve Gregory Lee, including:

   a. All records that relate to FEMA funds, FEMA regulations, training requirements, training certificates and creation of fraudulent training certificates and other efforts to obtain FEMA funds without complying with FEMA regulations.

   b. Any records including e-mail messages/correspondences, Internet sites, user names, user identification numbers, Internet provider information, writings, or communications, including letters, instant messages, or any type or correspondence which describes, displays images, or contains information or acts, memos in whole or in part, that relate to Gregory Lee and creation of fraudulent training certificates and other efforts to obtain FEMA funds without complying with FEMA regulations.

   c. Any record documented on any media, which appears to be a password, personal Identification number, items) and/or information used to access and/or facilitate access of said item(s), to be searched.

   d. Any record documented on any media, which establishes and/or tends to establish the state of mind, motives, actions, means and/or intentions of any persons with knowledge or apparent knowledge of the crime(s), including diaries, journals, audio and/or video recordings.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet to communicate with federal government servers, including:

   a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.